UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA
DE REDES DE COMPUTADORES

ANDRÉ RIBEIRO SOUTO

A Importância da Segurança Aplicada à Tecnologia VOIP

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. Dr. João Netto
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, dezembro de 2008.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

VOIP	VOICE OVER INTERNET PROTOCOL
SIP	*Session Initiation Protocol*
MCU	Multipoint Control Units
IP	Internet Protocol
PSTN	*Public Switched Telephone Network*
RTCP	*Real Time Control Protocol*
RTP	*Real Time Protocol*
TCP	*Transport Control Protocol*
UDP	*User Datagram Protocol*
SRTCP	Secure Real-Time Transport Control Protocol
RTCP	Real-Time Transport Control Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
IPsec	Internet Protocol Secuity
VLAN	*Virtual Local Área Network*
MIME	Multipurpose Internet Mail Extensions

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

A tecnologia VOIP se expande rapidamente e essa velocidade às vezes não é aliada com a segurança.

Nesta evolução das comunicações, destaca-se o protocolo SIP (*Session Initiation Protocol*), um protocolo capaz de iniciar, alterar e finalizar sessões multimídia, garantindo a convergência em definitivo, da telefonia tradicional para telefonia IP. Porém apesar das grandes vantagens trazidas pela convergência, esta trouxe também uma preocupação com segurança dos dados.

Implementações do protocolo SIP são vulneráveis a ataques comuns baseados em redes IP, bem como a ataques que são únicos ao SIP. Este fato coloca em risco as Informações das empresas que utilizam sistemas de telefonia IP. Ataques que fazem uso das vulnerabilidades do protocolo SIP, podem resultar na interrupção de aplicações fundamentais ao negócio de corporações sustentadas em uma rede Voip. Tal fato, dentro do contexto de concorrência global, tornará uma grande economia em sérios prejuízos.

Este trabalho irá apresentar algumas vulnerabilidades apresentadas no uso da tecnologia Voip e algumas ferramentas usadas para ataques ao protocolo SIP.

Palavras-Chave: VOIP, Ameaças, SIP, Ferramentas

The Importance of Security Technology Applied to Voip

ABSTRACT

The VOIP technology is rapidly expanding and with that speed sometimes is not allied with safety.

This evolution of communications, there is the protocol SIP (Session Initiation Protocol), a protocolable to initiate, amend and terminate multimedia sessions, ensuring convergence ultimately, the traditional telephony to IP telephony. But despite the great advantages brought by convergence, it also brought a new concern: the security of information, that requirement can confirm the maturity of the technology.

Implementations of the SIP protocol, are vulnerable to attacks based on common IP networks as well as the attacks that are unique to the SIP. This puts at risk the information systems of enterprises that use IP telephony. Attacks have made use of the vulnerabilities of the SIP protocol, can result in the interruption of basic applications to the business of corporations sustained in a VoIP network This fact, within the context of global competition, will make a big economy in serious damage.

This study aims to present some vulnerabilities presented in the use of VoIP technology and some tools used for attacks on the SIP protocol.

Keywords: VOIP, Threats, SIP, Tools

1 INTRODUÇÃO

A segurança é ponto fundamental e deve ser aplicada no uso da tecnologia Voip visando uma otimização no retorno da sua utilização.

A tecnologia Voip se expande rapidamente e essa velocidade às vezes não é aliada com a segurança. Voip é um assunto de grande importância na evolução dos serviços de telecomunicações; é necessário rever algumas questões fundamentais como a segurança das comunicações usando o SIP. Sendo assim, a segurança em sistemas baseados no protocolo SIP, torna-se um ponto importante a ser pesquisado, já que o mesmo já é um protocolo universal que integra a rede de voz e dados.

Como a tecnologia Voip dissemina-se rapidamente novas oportunidades de negócios surgem da sua utilização, como também novas vulnerabilidades da tecnologia aparecem.

Dessa forma este trabalho irá tratar da aplicabilidade da segurança na tecnologia Voip apresentando algumas vulnerabilidades dessa tecnologia e ferramentas a serem utilizadas.

1.1 Objetivo do Trabalho

Este trabalho tem como objetivo apresentar a importância da segurança aplicada a tecnologia Voip. Também objetiva apresentar algumas vulnerabilidades apresentadas no uso da tecnologia Voip e algumas ferramentas usadas para ataques ao protocolo SIP.

1.2 Organização do Texto

O trabalho é composto por 8 capítulos conforme divisão abaixo:

No primeiro capítulo apresenta-se a introdução do trabalho falando sobre seus objetivos e organização do texto.

No segundo capítulo é apresentado a tecnologia Voip e algumas de suas arquiteturas.

Já no terceiro e quarto capítulos são apresentados os Protocolos SIP e os Protocolos de Mídias.

No quinto capítulo é apresentado os Codecs e suas modalidades.

Em sequência, no sexto capítulo são apresentadas as vulnerabilidades da tecnologia Voip e no sétimo capítulo são apresentadas ferramentas e ameaças a tecnologia.

No oitavo capítulo são apresentadas as técnicas aplicadas a segurança do protocolo SIP.

Por último é apresentada a conclusão do trabalho e as referências bibliográficas.

2 A TECNOLOGIA VOIP

2.1 Visão geral sobre Voip

A tecnologia Voip (Voz sobre IP) vem para substituir a telefonia convencional. Enquanto a telefonia convencional utiliza à comutação de circuitos a tecnologia Voip utiliza a comutação de pacotes.

2.2 Arquitetura H323

A arquitetura H.323 é composta de quatro elementos principais, que são os terminais, gateways, gatekeepers e MCU´s, sendo os três primeiros denominados pela recomendação H.323 de pontos finais. Nesta arquitetura esses componentes podem rodar em um mesmo equipamento, o H323 é utilizada com mais freqüência devido a sua fácil interação com a rede de telefonia pública comutada. Figura 2.1 pode ver uma arquitetura H323.

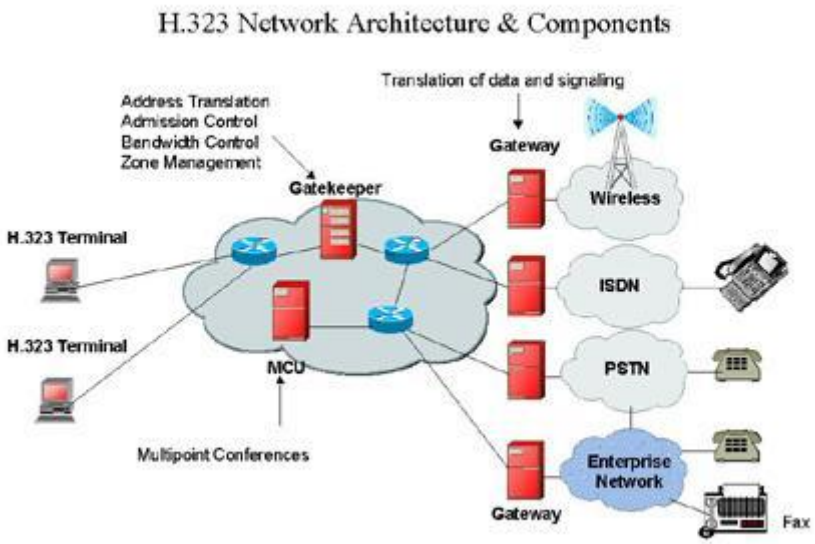

Figura 2.1:Arquitetura H323

Porém essa arquitetura apresenta uma complexidade e uma rigidez, que torna sua adaptação com aplicações futuras difícil.

Assim o IETF criou um comitê com objetivo de projetar uma nova arquitetura simples de fácil adaptação para as conferências de voip, arquitetura SIP.

2.3 Arquitetura SIP

Elementos que formam a arquitetura SIP, os quatro componentes principais dessa arquitetura na figura 2.2.

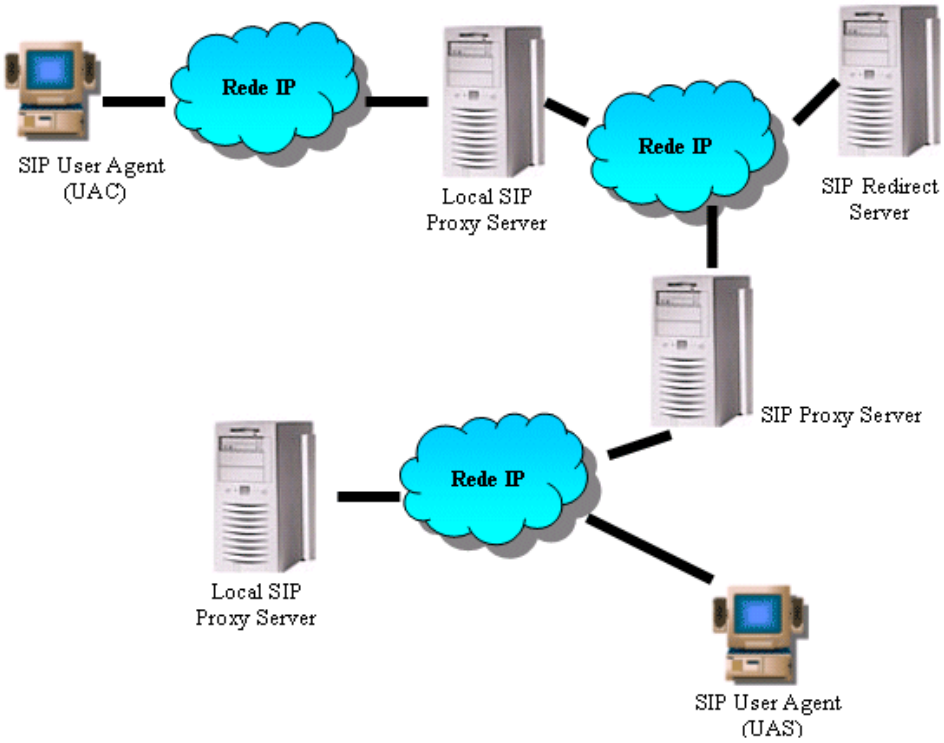

Figura 2.2:Arquitetura SIP

SIP User Agents- É a entidade do SIP que interage com o usuário. Possui a capacidade de enviar e receber requisições, assim, ele pode agir tanto como cliente (UAC), enviando requisições e recebendo respostas, ou como servidor (UAS), enviando respostas e recebendo requisições.

SIP Proxy Servers- É um tipo de servidor intermediário do SIP, que atua também como cliente e servidor, recebendo as requisições e passando adiante para servidores mais próximos do destino. Existem dois tipos de servidores Proxy, o Stateful Proxy Server e o Stateless Proxy Server. O Stateful Proxy Server mantém o estado das transações e permite dividir a chamada (Fork) para múltiplos servidores na tentativa de localizar o usuário, dessa maneira ele cria uma árvore de busca, possui maior confiabilidade, capacidade de computar o gasto do cliente e utilizam protocolo TCP. O Stateless Proxy Server não armazena o estado da transação apenas envia adiante as requisições e as respostas, possuem maior velocidade, porem menos confiabilidade e incapacidade de computar gastos do cliente.

SIP Redirect Server- É um tipo de servidor SIP, que responde ao pedido do UA fornecendo o nome e a localização do usuário, esse servidor não reencaminha os pedidos.

SIP Registrar Server- Servidor que armazena registros sobre usuários, fornecendo um serviço de localização.

O SIP funciona numa arquitetura cliente/servidor, e suas operações envolvem sessões de requisição e resposta do protocolo HTTP e no RTSP, os User Agents Client realizam perguntas e os User Agents Servers respondem a essas perguntas. Há 6 métodos de requisição que são: *INVITE, ACK, CANCEL, OPTIONS, REGISTER* e *BYE.*

INVITE- O método INVITE solicita o estabelecimento de uma sessão. O corpo do INVITE contem a descrição da sessão utilizando o SDP (Session Description

Protocol). Se um método INVITE for enviado durante a execução de uma sessão, ele é chamado de re-INVITE. Re-INVITE's geralmente são utilizados para mudar parâmetros da sessão;

ACK- O método ACK funciona como a confirmação de um INVITE, se o INVITE não contiver a descrição da sessão, o ACK deve conter;

CANCEL- O método CANCEL cancela todos os métodos pendentes de resposta;

OPTIONS- O método OPTIONS faz uma pergunta sobre as capacidades e disponibilidade das funcionalidades do receptor, a resposta contém uma listagem com os métodos, extensões e codecs suportados;

REGISTER- Um cliente usa este método para registrar o "alias" (apelido) do seu endereço em algum servidor SIP, que, por aceitar registro de usuários, chamamos de serviço REGISTRAR.

BYE- Usado para terminar uma sessão estabelecida.

As mensagens de resposta SIP formam um conjunto de códigos numéricos de resposta baseado no código de resposta do HTTP, elas são divididas em seis classes, veja tabela 2.1.

Provisório (1xx): Requisição em processo de conexão, em andamento;

Finalizadas (2xx, 3xx, 4xx, 5xx, 6xx): Indicam a conclusão da conexão SIP.

Tabela 2.1:Tabela de Códigos

Classe	**Tipo**	**Código**	**Status**
1xx	Informativo		Pedido Recebido, continuando o processamento do pedido
		100	Tentando
		180	Chamando
		181	A chamada está sendo retransmitida
		182	Colocado na fila
2xx	Sucesso		A ação foi recebida, entendida e aceita com sucesso
		200	OK
3xx	Redirecionamento		Uma ação adicional deve ser tomada para completar o pedido
		300	Múltiplas escolhas
		301	Movido permanentemente
		302	Movido temporariamente
		380	Serviço alternativo
4xx	Erro de Cliente		O pedido contém sintaxe inválida ou não pode ser efetuado neste servidor
		400	Pedido inválido
		401	Não autorizado
		402	Necessário pagamento
		403	Proibido

		404	Não encontrado
		405	Método não permitido
		406	Não aceitável
		407	Necessária autenticação do proxy
		408	Tempo para o pedido esgotado
		409	Conflito
		410	Não mais presente
		411	Necessário fornecer comprimento
		413	Corpo da mensagem de pedido muito grande
		414	URI do pedido muito grande
		415	Tipo de mídia não suportado
		420	Extensão inválida
		480	Temporariamente não disponível
		481	Transação ou leg de chamada não existe
		482	Laço (loop) detectado
		483	Excesso de segmentos (hops)
		484	Endereço incompleto
		485	Ambíguo
5xx			Erro de servidor
		500	Erro interno no servidor
		501	Não implementado
		502	Gateway inválido
		503	Serviço não disponível
		504	Tempo esgotado no gateway
		505	Versão SIP não suportada
6xx			Falha global
		600	Ocupado em todos os lugares
		603	Declínio
		604	Não existe em lugar nenhum
		606	Não aceitável

3 PROTOCOLO SIP

O SIP (Protocolo de iniciação de sessão) é um protocolo utilizado para estabelecer chamadas e conferências através de redes via IP, que atua na camada 7 do modelo OSI, a camada de aplicação. O protocolo SIP é um padrão da IETF (Internet Engineering Task Force).

O SIP foi desenvolvido e projetado para interagir com outros protocolos da Internet como TCP, UDP, TLS, IP, DNS e outros. Por esse motivo oferece grande estabilidade e flexibilidade.

Segundo a IETF, o SIP foi projetado tendo como foco a simplicidade, e, com um mecanismo de estabelecimento de sessão, ele apenas inicia, termina e modifica a sessão, o que o torna um protocolo que se adapta confortavelmente a diferentes arquiteturas. Ele oferece 6 tipos de serviços para iniciação e finalização de sessões multimídias, descritas abaixo:

Localização do Usuário- O SIP é responsável pela localização do terminal para estabelecer a conexão;
Disponibilidade do Usuário- Responsável por realizar a vontade do usuário em estabelecer uma sessão de comunicação;
Recursos do Usuário- Responsável pela determinação dos meios a serem utilizados;
Características da Negociação- Responsável pela negociação e acordo entre as partes, quanto às funcionalidades que serão compartilhadas;
Gestão da Sessão- Responsável por iniciar, terminar ou colocar em espera, sessões;
Modificar Sessão- Responsável por modificar uma sessão em andamento;

4 PROTOCOLOS DE MÍDIAS

4.1 Real-time Transport Protocol (RTP)

RTP transporta fim-a-fim pacotes mídias de áudio, vídeo, texto em outros, em tempo real, foi definido pela IEFT como um dos principais protocolos utilizados pelos terminais, em conjunto com RTCP.

O protocolo RTP não reserva recurso da rede e também não garante qualidade de serviço para transmissão em tempo real. O RTCP é o protocolo que monitora as entrega de dados, tem funções mínimas de controle e identificação.

4.2 Real-time transport control Protocol (RTCP)

O protocolo RTCP, definido também através da recomendação [RFC 3550] do IETF, é baseado no envio periódico de pacotes de controle a todos os participantes da conexão (chamada), usando o mesmo mecanismo de distribuição dos pacotes de mídia (Voz). Desta forma, com um controle mínimo é feita a transmissão de dados em tempo real usando o suporte dos pacotes UDP (para Voz e controle) da rede IP.

5 CODECS

Um Codec converte sinais analógicos em sinais digitais para transmissão de dados na rede.

ITU G.711 - 64 Kbps, baseado em amostra. Também conhecido por alaw/ulaw
GSM - 13 Kbps (full rate), quadros de 20ms
ITU G.729 - 8 Kbps, quadros de 10ms

5.1 Codec G.711

Embora formalmente seja normalizado, em 1988, o codec G.711 PCM é o mais antigo codec da telefonia digital. Inventado por Bell Systems e introduzida no início dos anos 70, o T1 redes digitais de um empregado de 8-bits descompactado Pulse Code Modulation, esquema de codificação com uma taxa de amostragem de 8000 amostras por segundo. Isto permitiu um (teórica) de banda máxima voz de 4000 Hz. Um T1 tronco transporta 24 canais digitais multiplexados PCM juntos. O padrão europeu melhorado E1 transporta 30 canais.

Existem duas versões: A-law e U-law. U-law padrão T1 utilizado na América do Norte e do Japão. O A-law padrão E1 usado no resto do mundo. A diferença está no método do sinal analógico sendo dividido. Em ambos os regimes, o sinal não é amostrado linearmente, mas em um padrão logarítmico.

Usando G.711 para Voip temos uma melhor qualidade na voz, esse codec transmite as ondas (dados) sem compressão, isto é, a taxa de amostragem não sofre redução ou perda de qualidade, e isto é essencial para utilização desse tipo de serviço via VoIP, é o mesmo codec usado pela rede PSTN e linhas ISDN, soa exatamente como usar um telefone normal ou RDIS. A desvantagem é que ele utiliza mais banda, em seguida, outros codecs, com até 84 Kbps incluindo todos TCP / IP por cima. No entanto, com o aumento da utilização da banda larga, isso não deve ser um problema.

5.2 Codec GSM

O original 'Full Rate' GSM também chamado de codec RPE-LTP (Regular Pulse Excitation Long-Term Prediction). Este codec utiliza a informação obtida com as amostras anteriores (esta informação não muda muito rapidamente), a fim de prever a atual amostra. O sinal de conversação é dividida em blocos de 20 MS. Esses blocos são passados para o codec, que tem uma taxa de 13 kbps, a fim de obter blocos de 260 bits.

Recentes sistemas GSM utilizam um par de novos codecs:

EFR (Enhanced Full Rate) uses ACELP (Algebraic Code Excited Linear Prediction)

HR (Half Rate) uses CELP-VSELP (Code Excited Linear Prediction - Vector Sum Excited Linear Prediction)

5.3 Codec G.729

O G.729 é um padrão ITU, é um algoritmo de compressão de dados para a voz que comprime áudio em pedaços de 10 milissegundos. Ou tons musicais, tais como tons DTMF ou fax só podem ser transportados com este Codec utilizando a RTP Payload para Dígitos DTMF, Telefonia Tons e sinais de Telefonia, conforme especificado no RFC 2833.

O G.729 é amplamente utilizado em Voz sobre IP (Voip) as suas aplicações tem uma exigência de baixa largura de banda . Norma G.729 funciona a 8 kbits/segundo, mas existem extensões, que também fornecem 6.4 kbits / segundo e 11,8 kbits/segundo para melhorar ou piorar respectivamente a qualidade de voz. Também é muito comum o codec G.729a que é compatível com G.729, porém exige menos computação. Essa menor complexidade não é gratuita uma vez que a qualidade de voz piora um pouco.

6 VULNERABILIDADES VOIP

A tecnologia Voip já esta presente em grande parte das empresas particulares e nos órgãos do governo.

Um dos grandes pontos positivos dessa solução em relação às redes PSTN (Telefonia de comutação de circuitos) e grande redução de custo de telefonia, e quando se pensou nessa tecnologia o que se levou mais em conta foi a interoperabilidade.

Com esse grande atrativo da tecnologia Voip muitos migram da telefonia de comutação de circuitos para telefonia de comutação de pacotes sem os devidos cuidados com a segurança, a solução que deveria reduzir custo, pode se tornar problemas de altos custos.

Se por um lado a empresa tem a uma redução de custos com as ligações telefônicas via internet, por outro, esta deixando o seu dados de voz exposto a pragas que hoje atacam a redes de dados, Worns, vírus, spam em Voip , ataque de negação de serviço e fraudes, assim comprometendo a infra-estrutura Voip.

Segundo Yoshioka (2003), existem alguns desafios a serem considerados em relação a segurança em telefonia IP:

a) Confidencialidade: As informações armazenadas e transmitidas são acessíveis somente aos autorizados.

b)Autenticidade: Assegurar a correta identificação da origem mensagem.

c) Integridade: Garantir que as mensagens não sejam apagadas ou alteradas de forma não autorizada.

d) Disponibilidade: As informações e serviços devem estar disponíveis 99,999%(Five nines) para os autorizados.

e) Não Repúdio: Garantir que originador e o receptor da mensagem não possam negar a autoria e recebimento respectivamente.

f) Controle de Acesso: O acesso às informações e recursos deve ser controlado por autorizados.

As redes Voip estão suscetíveis aos mais diversos tipos de ameaças. Um atacante pode conseguir acesso a servidores e captura informações vitais de uma empresa, ou

ainda empregar de forma maliciosa os serviços de voz, através do acesso não autorizado, beneficiando-se das vulnerabilidades do sistema.

Segundo Dhamankar (2004), falhas existentes nestes sistemas são definidas da seguinte forma:

a) Vulnerabilidades dos Sistemas Operacionais implementados nos dispositivos VoIP: Os dispositivos VoIP, tais como: IP Phones, Call Manager, Gateways, e Proxy Servers, herdam as mesmas vulnerabilidades dos Sistemas Operacionais ou firmware, implementados nos mesmos. Estes dispositivos são tipicamente desenvolvidos com os Sistemas Windows ou Linux, estes com diversas vulnerabilidades já exploradas. Portanto, não importa o quão uma aplicação VoIP seja ser segura, se o Sistema operacional estiver comprometido, seu serviço de telefonia IP estará em risco.

b) Configuração inadequada dos dispositivos VoIP: Em sua configuração padrão, muitos dispositivos de VoIP, expõem diversas portas UDP e TCP. Estas portas podem ser vulneráveis a ataques do tipo DoS, Buffer overflow, e ainda permitir que senhas fracas sejam facilmente capturadas.

c) Vulnerabilidades da infra-estrutura IP: O serviço de VoIP depende diretamente da disponibilidade da infra-estrutura IP em que este esteja implementado. Utilizando-se dos protocolos UDP e TCP, como meio de transporte, o serviço de VoIP, está suscetível as diversas ameaças tais como ataques de DDoS, SYN flood, que podem gerar indisponibilidade do serviço, ou ainda, ataques de hijaking no caso do TCP, e a fragmentação maliciosa, como o ping-da-morte (ping-of-death), no caso do UDP.

d) Vulnerabilidades em implementações de protocolos para VoIP: Os protocolos escritos para VoIP não tem como prioridade a segurança, e sim a interoperabilidade. Muitas vulnerabilidades encontradas em implementações destes protocolos, como o SIP é resultado de pesquisas de grupos especializados que geralmente disponibilizam suas ferramentas para teste das vulnerabilidades nas implementações dos protocolos.

e) Vulnerabilidades na camada de aplicação VoIP: Nesta camada existem uma variedade de ataques específicos ao VoIP. Incluído:

- Denial of Service (DoS)
- Call Hijacking
- Resource Exhaustion
- Evearsdropping
- Message Integrity

7 FERRAMENTAS E AMEAÇAS

7.1 Invite Flood

Invite - mensagem usada para iniciar uma chamada no servidor SIP.

O invite flood é um ataque que consiste em enviar milhares de mensagens ao servidor SIP para iniciar conexões. O ataque (TCP SYN FLOOD) ocorre quando um invasor envia múltiplas solicitações invite (TCP SYN) para um gateway Voip ou para o administrador de chamada do sistema, provocando um estado de esgotamento dos recursos na pilha TCP/IP do sistema. Com os recursos esgotados, o sistema está impossibilitado de aceitar novas requisições (Chamadas). Uma inundação de requisições (INVITE) é similar a um grande número de requisições legítimas, mas é falsa criando um excesso de iniciação de pedidos, causando um esgotamento dos recursos do servidor SIP.

Ferramentas usada para gerar Invite Flood:

IAXFLOODER

INVITE FLOODER

RTP FLOODER

SIPSAK

SIP SWISS ARMY KNIFE

7.2 Registration Hijack (seqüestro de registro)

Register - Registra um usuário em um servidor SIP

Registration Hijack é um tipo de ataque que seqüestra um registro de um usuário autentico, o atacante altera o registro do usuário valido, e faz se passar pelo usuário válido. Esse tipo de ataque normalmente acaba evoluindo para um ataque do tipo MITM Figura 7.1.

Ferramenta de Seqüestro de registro:

Registration Adder

Registration Eraser

Registration Hijacker

Reghijacker

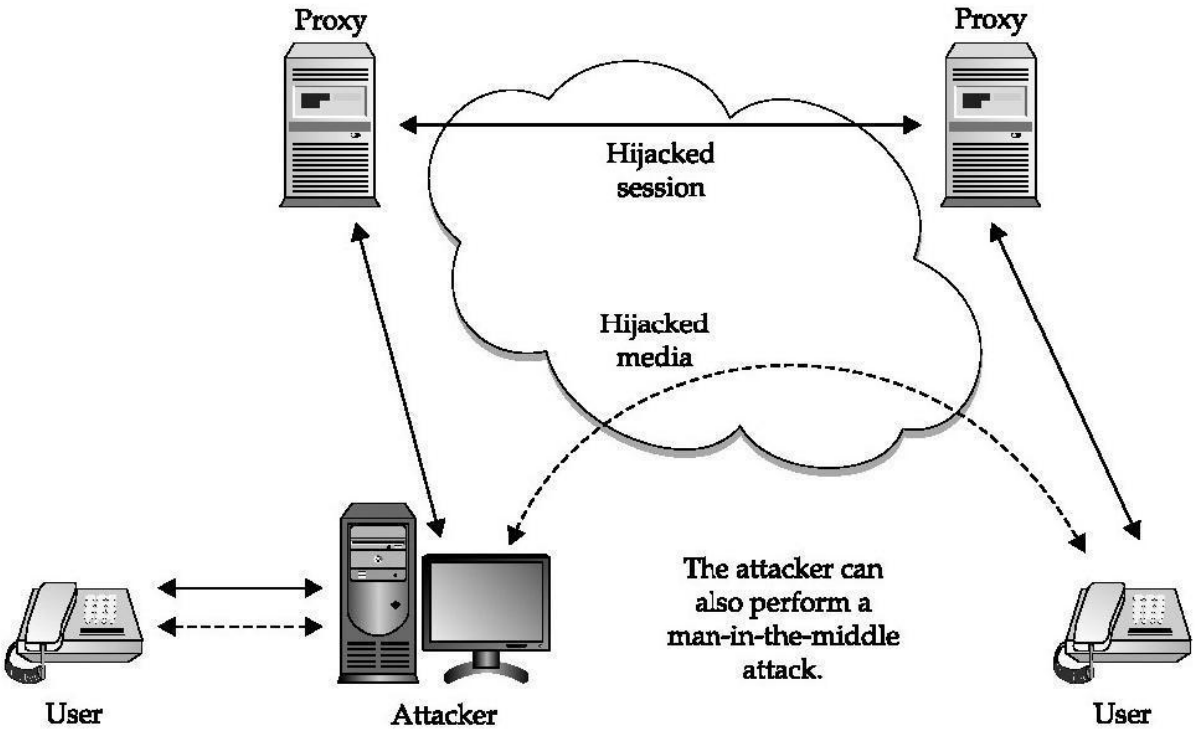

Figura 7.1: MITM

Tabela 7.1: Remoção de um Registro.

REGISTER sip: sip.my_proxy.com:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.1.56:5060 From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6 To: <sip:0987654321@sip.my_proxy.com> Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA CSeq: 500646445 REGISTER **Contact: <sip:654321@172.20.1.56:5060>** **Expires: 1800** User-Agent: VEGA400/10.02.07.2xS009 Content-Length: 0	REGISTRO VÁLIDO
REGISTER sip: sip.my_proxy.com:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.1.56:5060 From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6 To: <sip:0987654321@sip.my_proxy.com> Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA CSeq: 500646445 REGISTER **Contact: *** **Expires: *** User-Agent: VEGA400/10.02.07.2xS009 Content-Length: 0	REMOÇÃO DE UM REGISTRO

Tabela 7.2: Registro alterado.

REGISTER sip: sip.my_proxy.com:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.1.56:5060 From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6 To: <sip:0987654321@sip.my_proxy.com> Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA CSeq: 500646445 REGISTER **Contact: <sip:654321@172.20.1.56:5060>** **Expires: 1800** User-Agent: VEGA400/10.02.07.2xS009 Content-Length: 0	Registro Valido
REGISTER sip: sip.my_proxy.com:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.1.56:5060 From: <sip:0987654321@sip.my_proxy.com>;tag=0002-0000-D2C784D6 To: <sip:0987654321@sip.my_proxy.com> Call-ID: rE0x0001-0001-65C2F446-99@AAE2A42DF82D1D0AA CSeq: 500646445 REGISTER **Contact: sip:654321@172.20.1.101:5060 ← Registro Alterado** **Expires: 1800** User-Agent: VEGA400/10.02.07.2xS009 Content-Length: 0	Registro Falso

7.3 Call Eavesdropping (Escuta telefônica)

Call Eavesdropping é o método usado pelo atacante para monitorar toda a sinalização e o fluxo de dados. Pela escuta o atacante pode saber nomes de usuários, senhas e números de telefone, assim controlar o plano de chamadas, o voicemail, pode encaminhar chamadas.

Mais importante ainda, o atacante pode também ter acesso a informações pessoais e confidenciais das empresas pela escuta VoIP baseada em conversas reais.

Como ocorre a escuta telefônica:

1º Passo: Técnica Ataque do homem de meio (ARP POISONING)

Ferramentas:

- ETTERCAP
- PORT MIRRORING NO SWITCH

2º Passo: Ferramentas de filtragem de pacotes:

-WireShark
- Cain e Abel
- Vomit
- Voipong
- Oreka
- DTMF decoder

7.4 Fuzzing

Fuzzing é um método para encontrar erros e vulnerabilidades, o atacante cria diferentes tipos de pacotes especificamente para o protocolo que deseja atacar, leva em consideração às características do protocolo, o protocolo é testado até que ocorra uma falha, veja tabela 7.3.

Tabela 7.3: Fuzzing

INVITE sip:UserB@biloxi.com SIP/2.0 Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9 Max-Forwards: 70 From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl To: LittleGuy <sip:UserB@biloxi.com> Call-ID: 3848276298220188511@atlanta.com CSeq: 1 INVITE Contact: <sip:UserA@client.atlanta.com;transport=tcp> Content-Type: application/sdp Content-Length: 143	Mensagem Valida
INVITE sip:UserB@biloxi.com SIP/2.0 Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9 Max-Forwards: 70 From: BigGuy <sip:UserA@atlanta.com**xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx** **Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx** **Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx** **xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx**>;tag=9fxced76sl To: LittleGuy <sip:UserB@biloxi.com> Call-ID: 3848276298220188511@atlanta.com CSeq: 1 INVITE Contact: <sip:UserA@client.atlanta.com;transport=tcp> Content-Type: application/sdp Content-Length: 143	Mensagem Invalida

Ferramentas Fuzzing realiza mudanças no pacote:

- Asteróide
- Fuzzy Packet
- Mu Security VoIP Fuzzing Platform
- Ohrwurm
- PROTOS SIP Fuzzer
- SIP Forum Test Framework (SFTF)
- Sip-Proxy

7.5 SPIT (SPAM over Internet Telephony)

VoIP spam é uma ameaça relativamente nova com muitos poucos incidentes relatados até agora. Mesmo assim, cada conta VoIP tem um endereço IP associado a ele, permitindo que spammers enviem milhares de mensagens para os endereços IP-alvos. A maioria dessas mensagens acaba por lotar as caixas de voicemail, criando uma necessidade de ter uma maior capacidade de armazenamento de voz e também ferramentas eficientes que faça o gerenciamento das mensagens de voz.

Geralmente os *spams* têm caráter apelativo e na grande maioria das vezes são incômodos e inconvenientes veja figura 7.2.

Figura 7.2: SPIT

- Mensagens **não solicitadas** que chegam por meio de receptores de VoIP(softphones, aparelhos VoIP ou aparelhos convencionais utilizando ATA).

- Utilização em massa para trotes e telemarketing

- Mensagens indesejáveis em momentos indesejáveis com propostas indesejáveis de origens (geralmente) desconhecidas...

- Atrativo ao telemarketing convencional pela gratuidade, baixo custo do meio de transmissão e pelo número de funcionários.

Ferramenta: Spitter

8 MEDIDAS DE SEGURANÇA

8.1 Proteções da sinalização

Tem como objetivo proteger a sinalização voip de modo garantir a identidade dos remetentes e destinatários mantendo a:

-Confidencialidade: somente usuários autorizados acessam o que está armazenado ou sendo transmitido.

-Autenticidade: identificação da origem da mensagem, ou seja, se ela foi mesmo mandada pelo emissor correspondente ou é uma falsa mensagem de um atacante.

-Integridade: garantir que nada do que esteja armazenado seja modificado ou apagado sem autorização

-Disponibilidade: As informações e dados devem estar disponíveis aos usuários autorizados

-Não repúdio: o emissor não pode negar que enviou mensagens e o receptor não pode negar o recebimento da mesma

-Controle de acesso: deve ser o controle de quem tem acesso aos serviços, informações e recursos.

Para manter a garantia dessas questões, existem três técnicas usadas para o protocolo SIP:

-IPSEC : Fornece a capacidade de comunicação segura entre pontos com a implementação de protocolos IPSec.

-S/MIME: faz segurança de conteúdo, criptografando as mensagens SIP

-TLS: (Transport Layer Security) proporciona uma camada segura de transporte envolvendo TCP.

8.2 Proteções de Mídias

Para a proteção das mídias o protocolo foi criado o SRTP ele um padrão criado pelo IETF para garantir a confidencialidade e a integridade do áudio transportado pelo RTP, de modo que mesmo que o tráfego de áudio seja capturado por um terceiro, os dados sejam inúteis, pois não será possível remontar o áudio e ouvir a conversa sem a chave de criptografia.

Para o gerenciamento das chaves de criptografia, o SRTP utiliza o protocolo Multimedia Internet Keying (MIKEY), que utiliza o sistema de chaves précompartilhdas (pre-shared keys), infra-estrutura de chave pública e o algoritmo Diffie-Hellman para trocar as chaves.

Como o tráfego de áudio pode ser criptografado de ponta a ponta, ou seja de um telefone para o outro, o SRTP foi projetado para utilizar poucos recursos computacionais, já que geralmente um telefone IP possui um hardware simples.

Assim como o RTP, o SRTP possui um protocolo irmão, o SRTCP (Secure Real-Time Transport Control Protocol), utilizado para proteger o tráfego do RTCP (Real-Time Transport Control Protocol).

O algoritmo de criptografia utilizado pelo SRTP é o Advanced Encryption Standard (AES) de 128 bits, o que proporciona um nível de segurança elevado para o tráfego de áudio.

Para se evitar que o tráfego de voz seja capturado e utilizado por terceiros, devemos utilizar a criptografia no tráfego de áudio, ou seja, nos pacotes RTP e RTCP. Já para evitarmos a manipulação dos protocolos de sinalização, devemos também criptografar o tráfego de sinalização, impedindo assim a captura e modificação das mensagens de configuração de chamadas. Assim evitamos que um atacante engane os usuários enviando as chamadas feitas pelo mesmo para o lugar errado.

8.3 Segmentação da Rede

8.3.1 VLAN (Virtual Local Area Network)

VLAN como o nome diz, é uma rede virtual. A maioria dos switches atualmente é capaz de suportar a utilização de VLANs. Um VLAN segmenta um mesmo switch em diversas redes distintas, como se fossem redes físicas diferentes. Esta VLAN pode se estender por diversos switches diferentes, não precisando assim ficar isolada em cada switch.

A comunicação entre as VLANs deve ser feita por um dispositivo de camada 3, seja ele um roteador ou um switch com suporte à roteamento. O tráfego de voz deve ser separado do tráfego de dados através de VLANs, e a comunicação entre as duas redes deve ser restrita e controlada. Esta abordagem evita que problemas na rede de dados afetem o tráfego de voz.

Neste caso se um vírus comece a se disseminar entre os computadores da rede, o alto tráfego gerado por ele não afetará muito o tráfego de voz que está em uma rede separada.

Além de evitar que problemas na rede de dados afetem o tráfego de voz, a utilização de VLAN ajuda na implantação de mecanismos de qualidade de serviço, garantindo assim o desempenho necessário para as aplicações VoIP. A separação da

rede através de VLANs também dificulta a captura do tráfego de áudio ou de sinalização por parte dos atacantes.

8.4 Criptografia

Além de separar o tráfego de voz, é possível também criptografar o seu conteúdo, e assim, mesmo que um atacante consiga capturar os pacotes, o conteúdo dos pacotes continuará protegido.

Alguns equipamentos VoIP suportam a encriptação das mensagens utilizando o SRTP (Secure Real-time Transport Protocol) e o SRTCP (Secure Realtime Transport Control Protocol).

No caso dos equipamentos que não suportam o SRTP, pode-se encriptar o tráfego através da utilização do IPsec (Internet Protocol Security). Neste caso, a encriptação ocorre nos gateways com suporte a IPsec, como os concentradores de VPN (Virtual Private Networks).

8.5 Sobre o SPIT

O SPAM sobre a telefonia IP ainda não é um problema, já que hoje em dia não é muito fácil enviar ligações em massa, pois, diferentemente do envio de emails, isto ainda envolve um custo. Porém, o rápido desenvolvimento da tecnologia VoIP e sua maior adoção tornará o SPIT possível em breve, e medidas de prevenção estão sendo estudadas atualmente pelos fabricantes de equipamentos e softwares VoIP.

9 CONCLUSÃO

A utilização das redes de pacotes comutados para o tráfego de áudio é uma tendência que está cada vez mais se afirmando no mundo corporativo, bem como está chegando cada vez mais às residências de usuários domésticos, seja através de simples programas de computador como o Skype ou até equipamentos mais especializados para o VoIP como o ATA (Analog Telephony Adapter), que permite a utilização de um telefone comum para as ligações via internet. Importante ressaltamos também a fundamental necessidade da aplicação da segurança para a utilização do VoIP, tendo em vista que a expansão freqüente desta tecnologia trás consigo ameaças, que devem ser combatidas com o máximo de eficácia. Desta forma conclui-se que a segurança sobre sistemas VoIP será cada vez mais requisitada conforme o seu crescimento e expansão e o protocolo SIP conforme tema base do trabalho atualmente é um dos mais aptos para atingir todas estas expectativas, sejam elas corporativas, domesticas ou em qualquer outra área onde aplicações VoIP estiverem rodando.

REFERÊNCIAS

DHAMANKAR, R. **Intrusion Prevention**: The Future of VoIP Security. [S.l.]: Tipping Point Technology, 2004.

ENDLER, D.; COLLIER, M. **Hacking Voip Exposed**. Disponível em: < http://www.hackingvoip.com/sec_tools.html>. Acesso em: jun. 2008.

MEHTA, N. **How to protect your business from VoIP threats**. Disponível em: < http://www.scmagazine.com.au/feature/3272,how-to-protect-your-business-from-voip-threats.aspx>. Acesso em: ago. 2008.

PLEWES, A. **The biggest VoIP security threats - and how to stop them**. Disponível em: <http://www.silicon.com/research/specialreports/voipsecurity/0,3800013656,39166479,00.htm>. Acesso em: ago. 2008.

SPIT: Bringing Spam to Your Voicemail Box. Disponível em:< http://forwarding-international-numbers.tmcnet.com/feature/service-solutions/articles/4009-spit-bringing-spam-your-voicemail-box.htm>. Acesso em: jun. 2008.

THERMOS, P. **VoIP Security Threats, Vulnerabilities, Countermeasures, and Best Practices**. [S.l.]: Palindrome Technologies, 2008.

Voip-List. Disponível em:< http://www.voip-list.com/news/spit_voice_spam_Advertisement.html >. Acesso em: ago. 2008.

VOIP-NEWS. Disponível em: <http://www.voip-news.com/faq/voip-security-faq/> Acesso em: jun. 2008.

VOIPSA. Disponível em: <http://www.voipsa.org/Resources/tools.php#VoIP%20Fuzzing%20Tools>. Acesso em: ago. 2008.

YOSHIOKA, S. **Aspectos de Segurança para Telefonia IP utilizando o Protocolo SIP**. Campinas: UNICAMP, 2003.

ZAR, J. **VoIP Security and Privacy Threat Taxonomy**: Public Release 1.0. October 2005. Disponível em:< http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf>. Acesso em: ago. 2008.